IEEE HOME | SEARCH IEEE | SHOP | WEB ACCOUNT | CONTACT IEEE

IEEE

Membership Publications/Services Standards Conferences Careers/Jobs

IEEE Xplore®
RELEASE 1.6

Welcome
United States Patent and Trademark Office

Help FAQ Terms IEEE Peer Review

Quick Links

»

Welcome to IEEE Xplore®

- Home
- What Can I Access?
- Log-out

Tables of Contents

- Journals & Magazines
- Conference Proceedings
- Standards

Search

- By Author
- Basic
- Advanced

Member Services

- Join IEEE
- Establish IEEE Web Account
- Access the IEEE Member Digital Library

Your search matched **16** of **1008086** documents.
A maximum of **500** results are displayed, **50** to a page, sorted by **Relevance** in **Descending** or

Refine This Search:
You may refine your search by editing the current search expression or entering a new one in th box.

encryption <and> ('s box' <or> 's boxes' <or> substit Search

□ Check to search within this result set

Results Key:
JNL = Journal or Magazine **CNF** = Conference **STD** = Standard

1 **Avalanche characteristics of substitution-permutation encryption networks**
Heys, H.M.; Tavares, S.E.;
Computers, IEEE Transactions on , Volume: 44 , Issue: 9 , Sept. 1995
Pages:1131 - 1139

[Abstract] [PDF Full-Text (800 KB)] IEEE JNL

2 **Provable security of substitution-permutation encryption networks against linear cryptanalysis**
Keliher, L.; Meijer, H.; Tavares, S.;
Electrical and Computer Engineering, 2000 Canadian Conference on , Volume: 1 , 7-10 March 20
Pages:37 - 42 vol.1

[Abstract] [PDF Full-Text (472 KB)] IEEE CNF

3 **Construction of highly nonlinear injective S-boxes with application to CAST-like encr algorithms**
Youssef, A.M.; Chen, Z.G.; Tavares, S.E.;
Electrical and Computer Engineering, 1997. IEEE 1997 Canadian Conference on , Volume: 1 , 25 1997
Pages:330 - 333 vol.1

[Abstract] [PDF Full-Text (320 KB)] IEEE CNF

4 **On the security of the CAST encryption algorithm**
Heys, H.M.; Tavares, E.;
Electrical and Computer Engineering, 1994. Conference Proceedings. 1994 Canadian Conference on , 25-28 Sept. 1994
Pages:332 - 335 vol.1

[Abstract] [PDF Full-Text (260 KB)] IEEE CNF

5 **Transform domain analysis of DES**
Guang Gong; Golomb, S.W.;
Information Theory, IEEE Transactions on , Volume: 45 , Issue: 6 , Sept. 1999
Pages:2065 - 2073

[Abstract] [PDF Full-Text (208 KB)] IEEE JNL

6 **Integrating the Data Encryption Standard into Computer Networks**
Smid, M.;
Communications, IEEE Transactions on [legacy, pre - 1988] , Volume: 29 , Issue: 6 , Jun 1981

Pages:762 - 772

[Abstract] [PDF Full-Text (1136 KB)] **IEEE JNL**

---

7 **A single-chip FPGA implementation of the data encryption standard (DES) algorithm**
Wong, K.; Wark, M.; Dawson, E.;
Global Telecommunications Conference, 1998. GLOBECOM 98. The Bridge to Global Integration. IEEE , Volume: 2 , 8-12 Nov. 1998
Pages:827 - 832 vol.2

[Abstract] [PDF Full-Text (304 KB)] **IEEE CNF**

---

8 **Secure and fast encryption using chaotic Kolmogorov flows**
Scharinger, J.;
Information Theory Workshop, 1998 , 22-26 June 1998
Pages:124 - 125

[Abstract] [PDF Full-Text (248 KB)] **IEEE CNF**

---

9 **Large s-box design using a converging method**
Hendessi, F.; Gulliver, T.A.; Sheikh, A.U.H.;
Information Theory. 1997. Proceedings., 1997 IEEE International Symposium on , 29 June-4 July
Pages:177

[Abstract] [PDF Full-Text (132 KB)] **IEEE CNF**

---

10 **A method for obtaining cryptographically strong 8x8 S-boxes**
Xun Yi; Shi Xin Cheng; Xiao Hu You; Kwok Yan Lam;
Global Telecommunications Conference, 1997. GLOBECOM '97., IEEE , Volume: 2 , 3-8 Nov. 199
Pages:689 - 693 vol.2

[Abstract] [PDF Full-Text (472 KB)] **IEEE CNF**

---

11 **Message authentication with one-way hash functions**
Tsudik, G.;
INFOCOM '92. Eleventh Annual Joint Conference of the IEEE Computer and Communications Soci IEEE , 4-8 May 1992
Pages:2055 - 2059 vol.3

[Abstract] [PDF Full-Text (364 KB)] **IEEE CNF**

---

12 **Hardware implementation of 128-bit symmetric cipher SEED**
Young-Ho Seo; Jong-Hyeon Kim; Dong-Wook Kim;
ASICs, 2000. AP-ASIC 2000. Proceedings of the Second IEEE Asia Pacific Conference on , 28-30 . 2000
Pages:183 - 186

[Abstract] [PDF Full-Text (316 KB)] **IEEE CNF**

---

13 **Efficient 8-cycle DES implementation**
Young Won Lim;
ASICs, 2000. AP-ASIC 2000. Proceedings of the Second IEEE Asia Pacific Conference on , 28-30 . 2000
Pages:175 - 178

[Abstract] [PDF Full-Text (352 KB)] **IEEE CNF**

---

14 **A block cipher technique for security of data and computer networks**
Rahouma, K.H.;
Internet Workshop, 1999. IWS 99 , 18-20 Feb. 1999
Pages:25 - 31

[Abstract] [PDF Full-Text (596 KB)] **IEEE CNF**

---

15 **A new criterion for the design of 8x8 S-boxes in private-key ciphers**

Jianhong Xu; Heys, H.M.;
Electrical and Computer Engineering, 1997. IEEE 1997 Canadian Conference on , Volume: 1 , 25
1997
Pages:322 - 325 vol.1

[Abstract] [PDF Full-Text (316 KB)] **IEEE CNF**

---

16 **The improved data encryption standard (DES) algorithm**
Seung-Jo Han; Heang-Soo Oh; Jongan Park;
Spread Spectrum Techniques and Applications Proceedings, 1996., IEEE 4th International Sympc
on , Volume: 3 , 22-25 Sept. 1996
Pages:1310 - 1314 vol.3

[Abstract] [PDF Full-Text (472 KB)] **IEEE CNF**

Home | Log-out | Journals | Conference Proceedings | Standards | Search by Author | Basic Search | Advanced Search | Join IEEE | Web Account | New this week | OPAC Linking Information | Your Feedback | Technical Support | Email Alerting | No Robots Please | Release Notes | IEEE Online Publications | Help | FAQ| Terms | Back to Top

acm PORTAL

US Patent & Trademark Office

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

+encryption +"key expansion"

SEARCH

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Published since January 1947 and Published before September 2000
Terms used encryption key expansion

Found 1 of 98,357

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

□ Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 1 of 1

Relevance scale

1 Towards practical "proven secure" authenticated key distribution
Yvo Desmedt, Mike Burmester
December 1993 **Proceedings of the 1st ACM conference on Computer and communications security**

Full text available: pdf(382.53 KB) Additional Information: full citation, abstract, references, citings, index terms

Secure key distribution is a critical component in secure communications. Finding 'proven secure' practical key distribution systems is one of the major goals in cryptography. The Diffie-Hellman variants, a family of key distribution systems, achieve some of the objectives of this goal. In particular, the 'non-paradoxical' system (by Matsumoto-Takashima-Imai and Yacobi) is claimed to be secure against a known-key attack. In this paper we show that the argument used to prove this is ...

Results 1 - 1 of 1

Terms of Usage Privacy Policy Code of Ethics Contact Us

Useful downloads: Adobe Acrobat QuickTime Windows Media Player Real Player acm PORTAL

US Patent & Trademark Office

Subscribe (Full Service) Register (Limited Service, Free) Login

Search: ● The ACM Digital Library ○ The Guide

+encryption +randomization +weak 's box' 's boxes' substitutic SEARCH

THE ACM DIGITAL LIBRARY

Feedback Report a problem Satisfaction survey

Published since January 1947 and Published before September 2000
Terms used encryption randomization weak 's box' 's boxes' substitution

Found 58 of 98,357

Sort results by: relevance

Display results: expanded form

Save results to a Binder

Search Tips

□ Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 58

Result page: **1** 2 3 next

Relevance scale

1 On randomization in sequential and distributed algorithms
Rajiv Gupta, Scott A. Smolka, Shaji Bhaskar
March 1994 **ACM Computing Surveys (CSUR)**, Volume 26 Issue 1

Full text available: pdf(8.01 MB) Additional Information: full citation, abstract, references, citings, index terms

Probabilistic, or randomized, algorithms are fast becoming as commonplace as conventional deterministic algorithms. This survey presents five techniques that have been widely used in the design of randomized algorithms. These techniques are illustrated using 12 randomized algorithms—both sequential and distributed— that span a wide range of applications, including:primality testing (a classical problem in number theory), interactive probabilistic proof s ...

Keywords: Byzantine agreement, CSP, analysis of algorithms, computational complexity, dining philosophers problem, distributed algorithms, graph isomorphism, hashing, interactive probabilistic proof systems, leader election, message routing, nearest-neighbors problem, perfect hashing, primality testing, probabilistic techniques, randomized or probabilistic algorithms, randomized quicksort, sequential algorithms, transitive tournaments, universal hashing

2 Simple constant-time consensus protocols in realistic failure models
Benny Chor, Michael Merritt, David B. Shmoys
July 1989 **Journal of the ACM (JACM)**, Volume 36 Issue 3

Full text available: pdf(2.23 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Using simple protocols, it is shown how to achieve consensus in constant expected time, within a variety of fail-stop and omission failure models. Significantly, the strongest models considered are completely asynchronous. All of the results are based on distributively flipping a coin, which is usable by a significant majority of the processors. Finally, a nearly matching lower bound is also given for randomized protocols for consensus.

3 A randomized protocol for signing contracts
Shimon Even, Oded Goldreich, Abraham Lempel
June 1985 **Communications of the ACM**, Volume 28 Issue 6

Full text available: pdf(1.23 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Randomized protocols for signing contracts, certified mail, and flipping a coin are presented. The protocols use a 1-out-of-2 oblivious transfer subprotocol which is axiomatically defined.The 1-out-of-2 oblivious transfer allows one party to transfer exactly one secret, out of two recognizable secrets, to his counterpart. The first (second) secret is received with probability one half, while the sender is ignorant of which secret has been received.An implementation of ...

4 Crytographic limitations on learning Boolean formulae and finite automata
M. Kearns, L. G. Valiant
February 1989 **Proceedings of the twenty-first annual ACM symposium on Theory of computing**

Full text available: pdf(1.32 MB) Additional Information: full citation, references, citings, index terms

5 Multi-prover interactive proofs: how to remove intractability
Michael Ben-Or, Shafi Goldwasser, Joe Kilian, Avi Widgerson
January 1988 **Proceedings of the twentieth annual ACM symposium on Theory of computing**

Full text available: pdf(1.90 MB) Additional Information: full citation, abstract, references, citings, index terms

Quite complex cryptographic machinery has been developed based on the assumption that one-way functions exist, yet we know of only a few possible such candidates. It is important at this time to find alternative foundations to the design of secure cryptography. We introduce a new model of generalized interactive proofs as a step in this direction. We prove that all NP languages have perfect zero-knowledge proof-systems in this model, without making any intractability assumptions.

6 Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems
Oded Goldreich, Silvio Micali, Avi Wigderson
July 1991 **Journal of the ACM (JACM),** Volume 38 Issue 3
Full text available: pdf(3.04 MB) Additional Information: full citation, references, citings, index terms

Keywords: NP, cryptographic protocols, fault tolerant distributed computing, graph isomorphism, interactive proofs, methodological design of protocols, one-way functions, proof systems, zero-knowledge

7 Simple constant-time consensus protocols in realistic failure models (extended abstract)
Benny Chor, Michael Merritt, David B. Shmoys
August 1985 **Proceedings of the fourth annual ACM symposium on Principles of distributed computing**
Full text available: pdf(1.05 MB) Additional Information: full citation, references, citings, index terms

8 Computational learning theory: survey and selected bibliography
Dana Angluin
July 1992 **Proceedings of the twenty-fourth annual ACM symposium on Theory of computing**
Full text available: pdf(2.11 MB) Additional Information: full citation, references, citings, index terms, review

9 Cryptographic limitations on learning Boolean formulae and finite automata
Michael Kearns, Leslie Valiant
January 1994 **Journal of the ACM (JACM),** Volume 41 Issue 1
Full text available: pdf(2.28 MB) Additional Information: full citation, abstract, references, citings, index terms

In this paper, we prove the intractability of learning several classes of Boolean functions in the distribution-free model (also called the Probably Approximately Correct or PAC model) of learning from examples. These results are representation independent, in that they hold regardless of the syntactic form in which the learner chooses to represent its hypotheses. Our methods reduce the problems of cracking a number of well-known public-key cryptosystems to the l ...

10 Software protection and simulation on oblivious RAMs
Oded Goldreich, Rafail Ostrovsky
May 1996 **Journal of the ACM (JACM),** Volume 43 Issue 3
Full text available: pdf(3.44 MB) Additional Information: full citation, abstract, references, citings, index terms

Software protection is one of the most important issues concerning computer practice. There exist many heuristics and ad-hoc methods for protection, but the problem as a whole has not received the theoretical treatment it deserves. In this paper, we provide theoretical treatment of software protection. We reduce the problem of software protection to the problem of efficient simulation on oblivious RAM.A machine is oblivious if thhe sequence in wh ...

Keywords: pseudorandom functions, simulation of random access machines, software protection

11 Design of practical and provably good random number generators
William Aiello, Sivaramakrishnan Rajagopalan, Ramarathnam Venkatesan
January 1995 **Proceedings of the sixth annual ACM-SIAM symposium on Discrete algorithms**
Full text available: pdf(1.01 MB) Additional Information: full citation, references, citings, index terms

12 Toward a secure system engineering methodolgy
Chris Salter, O. Sami Saydjari, Bruce Schneier, Jim Wallner
January 1998 **Proceedings of the 1998 workshop on New security paradigms**

Full text available: pdf(858.86 KB) Additional Information: full citation, references, citings, index terms

[13] Oblivious transfer and polynomial evaluation □
Moni Naor, Benny Pinkas
May 1999 **Proceedings of the thirty-first annual ACM symposium on Theory of computing**

Full text available: pdf(956.48 KB) Additional Information: full citation, references, citings, index terms

[14] Algorithms on Stings, Trees, and Sequences: Computer Science and Computational Biology □
Dan Gusfield
December 1997 **ACM SIGACT News**, Volume 28 Issue 4

Full text available: pdf(1.20 MB) Additional Information: full citation

[15] The discrete log is very discreet □
A. W. Schrift, A. Shamir
April 1990 **Proceedings of the twenty-second annual ACM symposium on Theory of computing**

Full text available: pdf(992.98 KB) Additional Information: full citation, citings, index terms

[16] Optimal algorithms for Byzantine agreement □
Paul Feldman, Silvio Micali
January 1988 **Proceedings of the twentieth annual ACM symposium on Theory of computing**

Full text available: pdf(1.72 MB) Additional Information: full citation, abstract, references, citings, index terms

We exhibit randomized Byzantine agreement (BA) algorithms achieving optimal running time and fault tolerance against all types of adversaries ever considered in the literature. Our BA algorithms do not require trusted parties, preprocessing, or non-constructive arguments. Given private communication lines, we show that n processors can reach BA in expected constant time in a syncronous network if any <

[17] Testing problems with sub-learning sample complexity □
Michael Kearns, Dana Ron
July 1998 **Proceedings of the eleventh annual conference on Computational learning theory**

Full text available: pdf(1.68 MB) Additional Information: full citation, references, citings, index terms

[18] P = BPP if E requires exponential circuits: derandomizing the XOR lemma □
Russell Impagliazzo, Avi Wigderson
May 1997 **Proceedings of the twenty-ninth annual ACM symposium on Theory of computing**

Full text available: pdf(1.16 MB) Additional Information: full citation, references, citings, index terms

[19] Public-key cryptography and password protocols □
Shai Halevi, Hugo Krawczyk
August 1999 **ACM Transactions on Information and System Security (TISSEC)**, Volume 2 Issue 3

Full text available: pdf(275.84 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We study protocols for strong authentication and key exchange in asymmetric scenarios where the authentication server possesses ~a pair of private and public keys while the client has only a weak human-memorizable password as its authentication key. We present and analyze several simple password authentication protocols in this scenario, and show that the security of these protocols can be formally proven based on standard cryptographic assumptions. Remarkably, our analysis shows optimal re ...

Keywords: dictionary attacks, hand-held certificates, key exchange, passwords, public passwords, public-key protocols

[20] Public-key cryptography and password protocols □
Shai Halevi, Hugo Krawczyk
November 1998 **Proceedings of the 5th ACM conference on Computer and communications security**

Full text available: Additional Information:

pdf(1.28 MB) full citation, references, citings, index terms

Results 1 - 20 of 58 Result page: **1** 2 3 next

Non-patent literature search information - 2/27/04

09652157
Michael J. Simitoski
Michael.Simitoski@uspto.gov
(703) 305-8191

Google

key "expansion unit" encryption
key "expansion unit"
DES decryption diagram
DES decryption illustration
DES mangler
key (XOR OR "exclusive-or") (substitution OR "s-box") expansion (rotate OR rotation)
shift "relatively prime" bits
"DES" "key expansion" "same" (substitution OR "s-box" OR "s-boxes")

ACM

'same s box' 'same s boxes' 'same substitution tables'
+encryption +"key expansion"
+encryption +randomization +weak 's box' 's boxes' substitution

IEEE

('same s box' <or> 'same s boxes' <or> 'same substitution tables')
encryption <and> ('s box' <or> 's boxes' <or> substitution)

Applications/Patents from Inventor Search

6,049,611
6,009,174
6,550,009
09/638,616
6,570,989
6,304,657
09/694,925

L Number	Hits	Search Text	DB	Time stamp
1	1	("6478871").PN.	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/27 08:52
4	0	(add near (carry adj up)) and (random near2 generat$3) and @ad<19990831	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/27 09:14
5	0	(add near (carry adj up))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/27 09:14
6	96	"carry-up"	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/27 09:14
7	16	"carry-up" same (add addition subtract$3)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/27 09:15
10	11	("carry-up" same (add addition subtract$3)) and @ad<20000831	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/27 09:18
11	1	6683956.pn.	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/27 09:18
12	1	(("5442705").PN.) and add$7	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/02/27 09:25